IdentityHub

PKI for the Masses

rick@openfortress.nl

INTERNETWIDE.ORG

FileSender 2.0

- SURFnet's huge-file-exchange
- HTTP upload, Email notify, HTTP download
- Hosted in a trusted place (open source)
- Encryption to offload operator trust
  - Out-of-band password exchange
  - Could use a PKI
  - But PKI is difficult… or is it not?

INTERNETWIDE.ORG

PKI is Easy

gpg -r bakker@orvelte.nep -e geheim.txt

gpg --auto-key-locate nodefault,ldap -r bakker@orvelte.nep -e geheim.txt

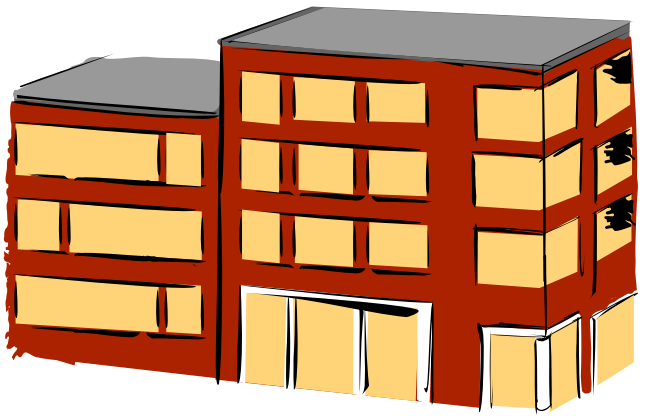
INTERNETWIDE.ORG

Control over Online Presence

- Domain for control over online identity
- Many open protocols are waiting to be deployed
- Control over
  - Identity
  - Security
  - Privacy, data
- So what went wrong?

INTERNETWIDE.ORG

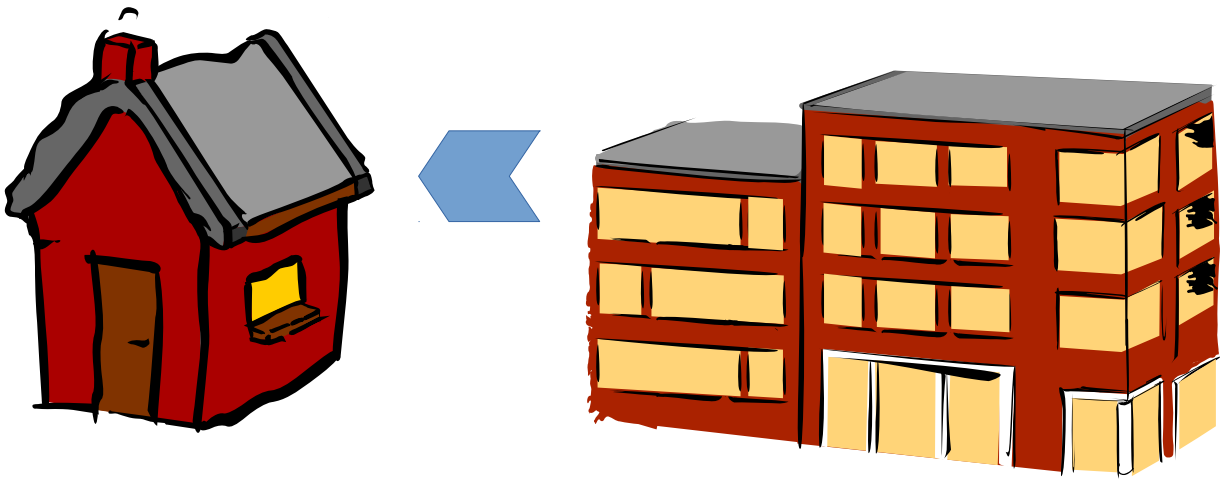
Hosting got Stuck



Multi-tenant Domain Hosting

INTERNETWIDE.ORG

Hosting got Stuck



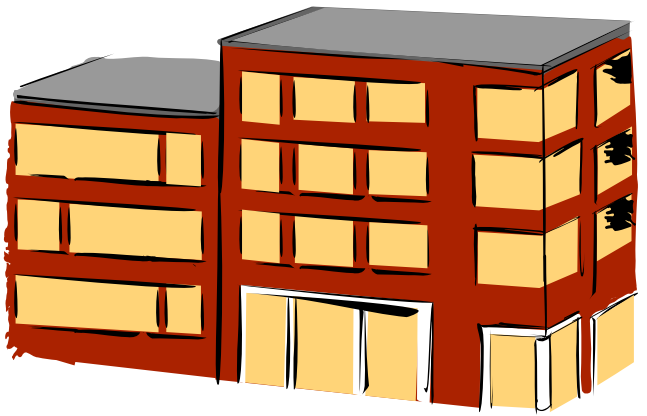
DIY

Multi-tenant Domain Hosting

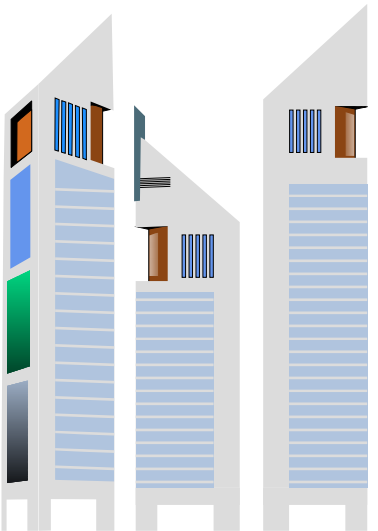
INTERNETWIDE.ORG

Hosting got Stuck

DIY



Multi-tenant Domain Hosting



GYM

INTERNETWIDE.ORG

Another Business Formula

- Two kinds of Hosting Provider
  - Identity Provider
  - Service Provider
- In this model, *it pays to specialise*
- Focus on *diversity* while maintaining *compatibility*
- **IdentityHub** for identity management
- **ServiceHub** for service plugins to identity mangement

INTERNETWIDE.ORG

Designing IdentityHub

- Open protocols (there are plenty)
- Hosting stack built on existing open source software
- Focus on central control

INTERNETWIDE.ORG

Designing IdentityHub

- Open protocols (there are plenty)
- Hosting stack built on existing open source software
- Focus on central control

- LDAP
  - Account/User Information
  - Automation-friendly data
- Kerberos

INTERNETWIDE.ORG

Designing IdentityHub

- Open protocols (there are plenty)
- Hosting stack built on existing open source software
- Focus on central control

- LDAP for Certificates, Public Keys, user's own `pkcs11:` URIs
- PKCS #11 for Private/Secret Keys
  - Remote and Managed
  - Personal and Group Credentials

INTERNETWIDE.ORG

Innovation in IdentityHub

- Kerberos is our “security foundation”
- User friendlyness: Single SignOn for all protocols

- Mobility & Security: Short-lived secrets
- Remote PKCS #11 is ASN.1 over GSSAPI

- TLS-KDH = TLS authentication with Kerberos tickets
- KXOVER = Kerberos realm crossover (“klaar-over”)

INTERNETWIDE.ORG

Innovation in IdentityHub

- Flexible Identities and ACLs for *all protocols*
- Services just follow the IdentityHub and use it

- Group Communication simplified
  - Email to group address: List Mail
  - WebDAV to group address: Shared Data
  - SIP calls to group address: Conferencing

INTERNETWIDE.ORG

About our Project

- InternetWide.org
  - blog, public face
- *.ARPA2.net
  - work packages, project documentation
- Funding
  - public sources: EZ, NLnet, SIDNfonds
- Collaborations
  - SURFnet, Hosting

INTERNETWIDE.ORG

IdentityHub

PKI for the Masses

rick@openfortress.nl

INTERNETWIDE.ORG